**AFFIDAVIT OF SPECIAL AGENT REMINGTON SCHILLING IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT**

I, Remington Schilling, being duly sworn, depose and state as follows:

1. I am a Special Agent with the United States Department of Veteran Affairs ("VA"), Office of the Inspector General ("VA OIG") and have been so employed since 2018. I am currently assigned to the Boston Resident Agency in Bedford, Massachusetts. Prior to joining the VA OIG, I was employed for approximately four years as a Special Agent with the U.S. Secret Service in Santa Ana, California. During my law enforcement career, I have received extensive law enforcement training. This training has included completing the Federal Law Enforcement Training Center's Criminal Investigator Training Program and the United States Secret Service Special Agent Training Course. More specifically, my law enforcement training has included training regarding various types of fraud, and theft of public money, property and records.

2. In addition to my training, I have experience in the investigation of various fraud schemes. I have participated in several fraud investigations as a case agent and in a subsidiary role. I have debriefed defendants, informants, and witnesses who had personal knowledge about fraud schemes and activities. I have participated in many aspects of fraud investigations, including the review of financial records, conducting surveillance, using confidential informants, and acting in an undercover capacity. During my law enforcement career, I have also participated in the preparation and/or execution of numerous search warrants.

3. I, along with the Social Security Administration's Office of Inspector General ("SSA OIG"), am investigating KAREN MARIE NOLAN ("NOLAN"), a

former employee assigned to the VA Medical Center located in Brockton, Massachusetts ("Brockton VA"), for theft of public money, in violation of 18 U.S.C. § 641, and for making materially false, fictitious, or fraudulent statements, in violation of 18 U.S.C. § 1001(a)(2).

4. This affidavit is made in support of an application for a warrant to search NOLAN'S business, Skin and Within, located at 146 Main Street, Suite 2B, Norfolk, Massachusetts 02056 (the "Target Premises"), as more fully described in *Attachment A*, because there is probable cause to believe that this location contains evidence, fruits, and instrumentalities of the crimes listed above, as described in *Attachment B*.

5. The facts contained in this affidavit are based upon information I have gained from my investigation, to include my personal observations, my review of records, my training and experience, and information obtained from other agents and witnesses. Because this affidavit is submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe are relevant to the issue of whether probable cause exists to search 146 Main Street, Suite 2B, Norfolk, Massachusetts 02056.

## *PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED*

### Background of the Investigation

6. NOLAN was hired by the VA on October 16, 2016, as a Nurse Practitioner of dermatology at the Brockton VA Campus. On August 8, 2017, NOLAN filed a claim for workers' compensation benefits under the Federal Employees' Compensation Act, claiming that she injured both wrists and her back at work on July 20,

2017. Her claim for workers' compensation benefits was approved and she received her first payment in November 2017.

7. On May 15, 2019, VA OIG received an allegation that NOLAN was defrauding the VA through the U.S. Department of Labor's ("DOL") Office of Workers' Compensation Program ("OWCP"). Specifically, it was alleged that NOLAN, despite claiming total disability as a result of her work injury in July 2017, was working at Skin and Within as a Nurse Practitioner.

8. Skin and Within is a skincare clinic located at 146 Main Street, Suite B, in Norfolk, Massachusetts. The clinic's website, https://skinandwithin.com/, lists NOLAN as one of the clinic's Board-Certified Nurse Practitioners.[1]

**Records Associated with NOLAN'S Claim for Workers' Compensation Benefits**

9. In furtherance of this investigation, I conducted a review of NOLAN'S VA employment records and records related to her reported on-the-job injury. Those records include four *DOL Form CA-1032: Request for Information on Earnings, Dual Benefits, Dependents, and Third-Party Settlements* ("DOL CA-1032"). A DOL CA-1032 form is an annual request by the DOL for OWCP benefit recipients to disclose all employment for which the recipient received any salary wages, income, sales commissions, piecework, or payment of any kind. Recipients also are required to disclose volunteer work for which any form of monetary or in-kind compensation was received. An OWCP

[1] The website also identifies a doctor, another nurse practitioner, a massage therapist, and an acupuncturist as individuals affiliated with Skin and Within. With the exception of the massage therapist, none of these individuals have been observed by agents to be present at the clinic.

benefit recipient is required to complete a DOL CA-1032 on an annual basis and submit the form to DOL OWCP in the month of the recipient's date of birth.

10. On May 15, 2018, NOLAN completed a DOL CA-1032 in support of her claim for federal workers' compensation benefits. On the DOL CA-1032, NOLAN claimed she was employed at the Brockton VA from October 2016 to July 20, 2017, and she was employed at Skin and Within from May 2012 to July 20, 2017.

11. On May 17, 2019, NOLAN filed a second DOL CA-1032 form in support of her federal workers' compensation claim. On the DOL CA-1032, NOLAN claimed that for the past fifteen months, she had not been employed, involved with any business enterprise, or conducted any volunteer work for which any form of monetary or in-kind compensation was received.

12. On May 24, 2020, and May 16, 2021, NOLAN filed additional DOL CA-1032 forms in support of her claim for federal workers' compensation benefits. Again, NOLAN reported that she had not been employed, involved with any business enterprise, or conducted any volunteer work for which any form of monetary or in-kind compensation was received in the past fifteen months. NOLAN wrote that she was now receiving monthly Social Security Administration ("SSA") Disability Payments.

**Records from the Insurance Fraud Bureau of Massachusetts**

13. A National Provider Identification ("NPI") number is a Health Insurance Portability and Accountability Act ("HIPPA") administrative simplification standard. The NPI is a unique, ten-digit identification number for covered health care providers. Covered health care providers and all health plans and health care clearinghouses must

use NPIs in the administrative and financial transactions adopted under HIPAA. NOLAN'S assigned NPI number is xxxxxx8196.

14. When a healthcare provider files a claim with a healthcare insurance company, the healthcare provider must provide the customer's information, customer's policy number, billing provider's information, date of medical service, the rendering provider's NPI, Current Procedural Treatment ("CPT") code, and CPT code description.

15. The Insurance Fraud Bureau ("IFB") of Massachusetts was contacted as part of the investigation into NOLAN and her work activities at Skin and Within. At the VA OIG's request, the IFB obtained insurance claims from the four major insurance companies in Massachusetts (Blue Cross Blue Shield, Harvard Pilgrim Healthcare, Aetna, and Tufts) submitted under NOLAN'S unique NPI number.

16. Information obtained from the IFB shows that NOLAN submitted claims to health insurance companies using her unique NPI number as the Service Provider, with KMN Dermatology and Aesthetics, P.C., and Skin and Within as the Billing Providers from the date of her alleged work injury, July 20, 2017, through July 21, 2021. A review of the National Plan and Provider Enumeration System ("NPPES") revealed that the NPI number for KMN Dermatology and Aesthetics, P.C., and Skin and Within is the same; KMN Dermatology and Aesthetics, P.C., is doing business as Skin and Within.[2] The address associated with the NPI number for KMN Dermatology and Aesthetics, P.C.,

[2] The NPI number assigned to KMN Dermatology and Aesthetics, P.C., d/b/a Skin and Within is xxxxxx5473. The Massachusetts Secretary of State, Corporations Division identifies NOLAN as the President, Treasurer, Secretary, and Director of KMN Dermatology and Aesthetics, P.C.

d/b/a Skin and Within is that of the Target Premises, 146 Main Street, Suite 2B, Norfolk, Massachusetts 02056.

17. IFB provided the VA OIG with information relating to insurance claims filed under NOLAN'S NPI from July 20, 2017, to July 21, 2021. The Billing Provider's Information for all of the claims filed under NOLAN'S NPI number from July 20, 2017, to July 21, 2021, is Skin and Within and KMN Dermatology and Aesthetics, P.C.

18. Starting from the date of NOLAN'S alleged injury at the VA, July 20, 2017, and continuing to July 21, 2021, KMN Dermatology and Aesthetics, P.C., and Skin and Within billed approximately 3,903 claims with NOLAN'S NPI listed as the rendering healthcare provider. The CPT codes and CPT code descriptions associated with the 3,903 claims include, but are not limited to, the following:

a. Office or other outpatient visit for the evaluation and management of an established patient, which requires a medically appropriate history and/or examination and low level of medical decision making. Ranging from 15 – 44 minutes;

b. Destruction (e.g., laser surgery, electrosurgery, cryosurgery, chemosurgery, etc.) of premalignant lesion;

c. Incision and drainage of abscess;

d. Injections, intralesional; up to and including 7 lesions;

e. Acne Surgery (e.g., marsupialization, opening of removal of multiple milia, comedones, cysts, pustules);

f. Biopsy of Skin, subcutaneous tissue and/or mucous membrane unless otherwise listed; each separate/additional lesion;

g. Excision, benign lesion including margins, except skin tag, scalp, neck, hands, feet, genitalia, diameter 0.5cm of less; and,

h. Tangential biopsy of skin (e.g., shave, scoop, saucerize, curette) single/additional lesion.

19. Based on the IFB's records, from July 20, 2017 to July 21, 2021, KMN Dermatology and Aesthetics, P.C., and Skin and Within billed an approximate total of $985,996.81 associated with NOLAN'S NPI number. Approximately $175,369.99 was paid during this time period.

**Bank Records**

20. As part of this investigation, records were obtained from Bank of America relating to a bank account held by NOLAN bearing account number xxxx xxxx 8691. These records show the deposit of United States Treasury checks made payable to NOLAN for workers' compensation benefits as well as the direct deposit of workers' compensation benefits for NOLAN by the United States Treasury.

21. In addition to the deposit of the federal benefits, records showed approximately nine direct deposit payments from Skin and Within into account xxxx xxxx 8691 from June 30, 2017, to October 20, 2017.

22. Approximately twelve checks bearing the name "Skin and Within Operating Account" and the address of the Target Premises were deposited into NOLAN'S account at Bank of America. The checks, drawn on Citizens Bank, were made payable to "Cash" or "Karen NOLAN." All of the checks were endorsed with the signature of "Karen NOLAN."

23. Approximately eight checks bearing the name "Skin and Within" and the

address of the Target Premises were deposited into NOLAN'S account at Bank of America. The checks, drawn on Santander Bank, were made payable to "Cash" or "Karen NOLAN." Each check bore the signature of "Karen NOLAN" and was endorsed by "Karen NOLAN."

**Surveillance**

24. On February 8, 2019, February 13, 2019, and February 20, 2019, surveillance was conducted of NOLAN at Skin and Within. On February 8, 2019, NOLAN was observed as she exited her vehicle and ascended the steps to Skin and Within while carrying a bag on her right shoulder and two bags in her right hand. She was not using any assistive devices. NOLAN remained inside Skin and Within from approximately 9:50 a.m. to approximately 4:19 p.m., when she exited the building and walked to her vehicle, again carrying a bag on her right shoulder and two bags over her right forearm.

25. On February 13, 2019, NOLAN was observed as she entered Skin and Within at approximately 1:02 p.m. carrying a purse and a bag. She exited the building at approximately 7:50 p.m., carrying two bags over her left forearm, and descended the steps to the parking lot. She walked to her vehicle and drove away.

26. On February 20, 2019, NOLAN was observed as she arrived at Skin and Within at approximately 12:28 p.m., exited her vehicle, and walked toward the building while carrying a large purse in her right hand. She ascended the steps without using the handrail and entered Skin and Within. NOLAN exited Skin and Within at approximately 7:54 p.m. She had her purse hanging over her left forearm. She descended the steps,

initially holding the handrail and then letting go. NOLAN walked to her vehicle and drove away.

27. On four occasions between December 2020 and January 2021, NOLAN was observed as she entered Skin and Within and departed several hours later. On each of those occasions, NOLAN carried a bag on her right shoulder and another bag in her left hand. She ascended and descended the stairs to Skin and Within without difficulty and did not use any assistive device. On December 14, 2020, before entering Skin and Within, NOLAN stacked several plastic chairs located on the deck outside of the business, picking them up with both hands, lifting them to shoulder height, then stacking them on top of each other. She did not demonstrate any difficulty when performing this task.

28. Based on all of the foregoing, I submit there is probable cause to believe that NOLAN violated 18 U.S.C. § 641, theft of public money, because she is performing work activity while receiving federal workers' compensation benefits. I also submit there is probable cause to believe that NOLAN violated 18 U.S.C. § 1001(a)(2), making materially false, fictitious, or fraudulent statements, because she is receiving benefits based on her false representations on four DOL CA-1032s that she has not been employed, involved with any business enterprise, or conducted any volunteer work for which any form of monetary or in-kind compensation was received since the date of her alleged work injury, July 20, 2017.

***THE PREMISES CONTAINS EVIDENCE, FRUITS, AND INSTRUMENTALITIES***

29. I also have probable cause to believe that the Target Premises to be searched contains fruits, evidence, and instrumentalities of violations of the federal statutes listed above, as described in *Attachment B*.

30. As noted in paragraph 16, above, information obtained from the IFB shows that NOLAN submitted claims to health insurance companies using her unique NPI number as the Service Provider, with KMN Dermatology and Aesthetics, P.C., and Skin and Within as the Billing Providers. The NPI number for KMN Dermatology and Aesthetics, P.C., and Skin and Within is the same, and the address associated with that NPI number is that of the Target Premises, 146 Main Street, Suite 2B, Norfolk, Massachusetts 02056.

31. As noted in paragraphs 22 and 23, above, checks bearing the name "Skin and Within Operating Account" and "Skin and Within" were deposited into NOLAN'S account at Bank of America. The listed address printed on those checks is the same address as the Target Premises: 146 Main Street, Suite 2B, Norfolk, Massachusetts 02056.

32. As outlined above, since 2019, investigators have observed NOLAN arriving and departing from the Target Premises at various times throughout the day, on multiple days per week. Investigators have also observed NOLAN inside the Target Premises and have observed a staff member inside the Target Premises booking appointments for clients on behalf of NOLAN.

33. On April 15, 2021, while conducting surveillance at the Target Premises, I used a Massachusetts Department of Motor Vehicle photo to identify NOLAN at the

Target Premises. I watched NOLAN park a white Subaru Forester, Massachusetts License Plate 5JG 367, in the parking lot outside of the Target Premises. Massachusetts Department of Motor Vehicle records identified the Subaru Forester with Massachusetts License Plate 5JG 367 as registered to NOLAN. I observed as NOLAN exited the vehicle and entered the rear entrance of the Target Premises.

34. On May 12, 2021, while conducting surveillance at the Target Premises, I observed as NOLAN and an unknown individual exited the rear entrance of the Target Premises. NOLAN walked to a white Subaru Forester, with Massachusetts License Plate 5JG 367, entered the vehicle, and drove away.

***SEIZURE OF COMPUTER EQUIPMENT AND DATA***

35. Based upon my investigation, and my training and experience, I believe that Skin and Within operates from 146 Main Street, Suite 2B, Norfolk, Massachusetts. As such, any business records, receipts, inventory, invoices, notes, and ledgers will be maintained there. These records could be maintained as either printed, paper files or electronic records maintained on computers, tablets, DVD's, thumb drives, portable hard drives or other forms of electronic media. I have specific reason to believe that the records will exist, in part, in digital format because investigators observed a staff member accessing a computer to book appointments.

36. From my training, experience, and information provided to me by other agents, I am aware that businesses frequently use computers to carry out, communicate about, and store records about their business operations. These tasks are frequently accomplished through sending and receiving business-related email and instant messages; drafting other business documents such as spreadsheets and presentations; scheduling

business activities; keeping a calendar of business and other activities; arranging for business travel; storing pictures related to business activities; purchasing and selling inventory and supplies online; researching online; and accessing banking, financial, investment, utility, and other accounts concerning the movement and payment of money online.

37. From my training, experience, and information provided to me by other agents, I am aware that businesses commonly store records of the type described in Attachment B in computer hardware, computer software, smartphones, and storage media.

38. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating

system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that

show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a

residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone

with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about

how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

j. In addition, based on my knowledge, training, and experience, I know that businesses and businesspeople often retain correspondence, financial, transactional, and other business records for years to identify past customers and vendors for potential future transactions; keep track of business deals; monitor payments, debts, and expenses; resolve business disputes stemming from past transactions; prepare tax returns and other tax documents; and engage in other business-related purposes. Here, NOLAN is believed to have been engaged in criminal activity for an extended period of time, since July 2017.

39. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from

accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer

> software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

40. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

41. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B because they are associated with the target. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

42. In this case, I recognize that Skin and Within is a functioning company that may perform some legitimate business functions, and that seizing computer equipment may have the unintended and undesired effect of limiting the company's ability to function.

a. As stated above, there are a variety of reasons why law enforcement agents might need to seize the computer equipment for subsequent processing elsewhere. If Skin and Within requires access to data that is not contraband or evidence of a crime, the government will work with the company after the search to copy this data onto storage media provided by the company for the company's use.

b. If the search team determines that there is no reason to seize certain of Skin and Within's computer equipment during the execution of this warrant, the team will create an onsite electronic "image" of those parts that are likely to store data specified in the warrant, if imaging is practical. Generally speaking, imaging is the taking of a complete electronic picture of the data, including all hidden sectors and deleted files. Imaging permits the agents to obtain an exact copy of the computer's stored data without actually seizing the computer equipment. However, imaging at the premises can often be impractical, because imaging is resource-intensive: it can take hours or days, thus requiring law enforcement agents to remain at the premises for much longer than they would remain if they seized the items, and it can require personnel with specialized experience and specialized equipment, both of which might be unavailable. If law

enforcement personnel do create an image at the premises, they will then search for the records and data specified in the warrant from the image copy at a later date off-site.

43. This warrant authorizes a review of electronic storage media, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the VA OIG may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

## CONCLUSION

44. Based on the information described above, I have probable cause to believe that NOLAN has violated 18 U.S.C. § 641 and 18 U.S.C. § 1001(a)(2).

45. Based on the information described above, I also have probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described in *Attachment B*, are contained within the premises described in *Attachment A*.

Sworn to under the pains and penalties of perjury.

Remington Schilling
Special Agent
Department of Veterans Affairs
Office of Inspector General

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on August 4, 2021.

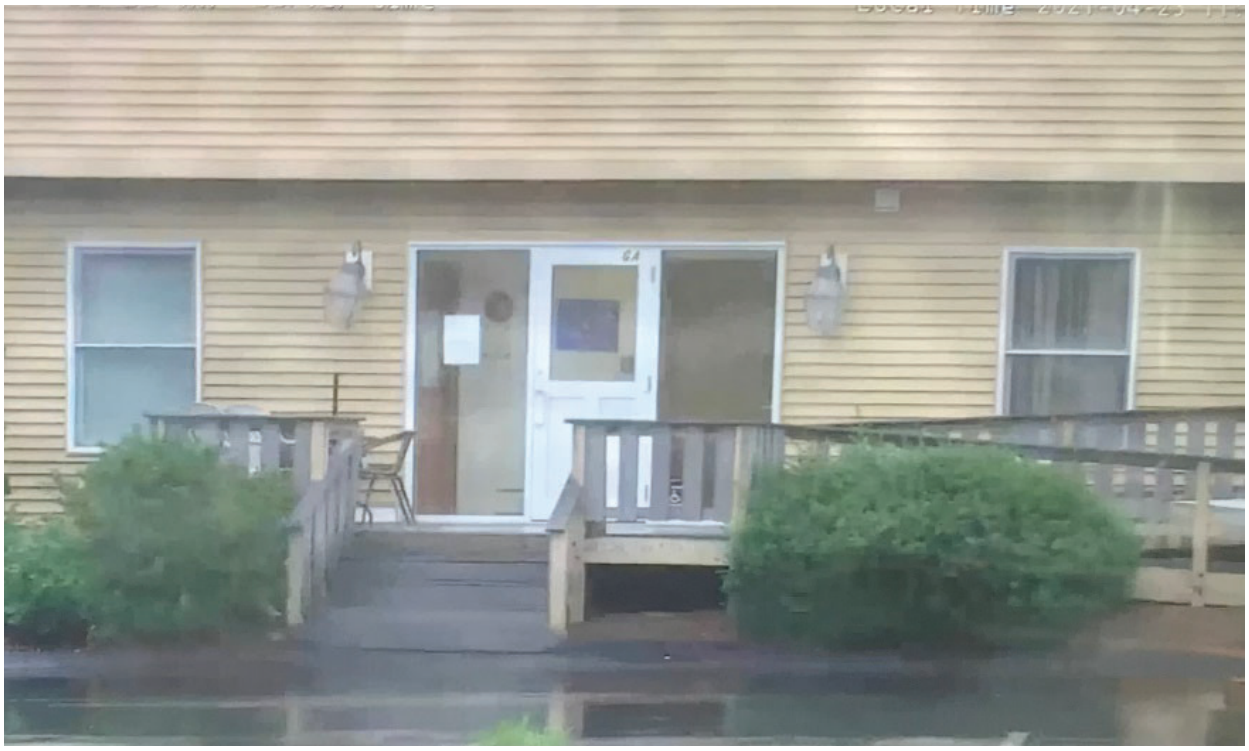
HONORABLE JENNIFER C. BOAL
UNITED STATES MAGISTRATE JUDGE

# ATTACHMENT A

## DESCRIPTION OF THE PREMISES TO BE SEARCHED

The premises to be searched is located at 146 Main Street, Suite 2B, Norfolk, Massachusetts. The building at 146 Main Street, Norfolk, Massachusetts 02056 is a two-story, tan building with two large windows on the first floor in the front. The window to the right of the front entrance bears lettering that reads "Skin & Within." There is a small vestibule upon entering the building through the front door on the first floor, with a door to the left and a door to the right. The door located on the right side of the vestibule displays a sign reading "Skin & Within."

Front Entrance



Rear Entrance

# ATTACHMENT B

## ITEMS TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. § 641 and 18 U.S.C. § 1001, for the period January 1, 2017, through the present, including, without limitation:

A. Records and tangible objects pertaining to the following people, entities, bank accounts, websites, and e-mail addresses:

1. Karen NOLAN;
2. United States Department of Veteran Affairs, Boston Healthcare System;
3. United States Department of Veteran Affairs, Brockton Medical Center;
4. Skin and Within;
5. KMN Dermatology and Aesthetics, P.C.;
6. karen@skinandwithin.com;
7. www.skinandwithin.com;
8. Santander Bank (account number xxxxxx6748);
9. Citizens Bank (account numbers xxxxxx1529, xxxxxx1537, and xxxxxx1545);
10. Bank of America (account numbers xxxx xxxx 8691, xxxx xxxx 8691, and xxxx xxxx 9210);
11. Square, Inc.;
12. Worldpay Bank Card;
13. Total System Services, Inc.;
14. CBMS Bank Card; and

15. "Worldpay Dlyentries."[3]

B. Records and tangible objects pertaining to the following topics:

1. NOLAN'S calendar and/or schedule at Skin and Within;

2. NOLAN'S performance of (medical/aesthetic/etc procedures) at Skin and Within;

3. Receipts, invoices, and payments for services rendered by NOLAN;

4. Insurance claims filed under NOLAN'S NPI number, xxxxxx8196; and

5. Receipts, invoices, and payments for Skin and Within gift cards sold.

C. Records and tangible objects pertaining to the payment, receipt, transfer, or storage of money or other things of value by Skin and Within or any one of the names listed above, including, without limitation:

1. Bank, credit union, investment, money transfer, and other financial accounts;

2. Credit and debit card accounts;

3. Tax statements and returns;

4. Business or personal expenses;

5. Income, whether from wages or investments; and

6. Loans.

D. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that

[3] Records obtained from Skin and Within's Merchant Services account at Citizens Bank reveal deposits from Square, Inc., Worldpay Bank Card, Total Systems Services, Inc., CBMS Bank Card, and "Worldpay Dlyentries."

might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;

2. evidence of computer software that would allow others to control the items, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the attachment of other computer hardware or storage media;

4. evidence of counter-forensic programs and associated data that are designed to eliminate data;

5. evidence of the times the computer equipment was used;

6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and

7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.

E. Records and tangible objects relating to the ownership, occupancy, or use of the premises to be searched (such as utility bills, phone bills, rent payments, mortgage payments, photographs, insurance documentation, receipts and check registers).

II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

**DEFINITIONS**

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer

software, computer-related documentation, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Computer-related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

F. "Data" means all information stored on storage media of any form

in any storage format and for any purpose.

G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

**RETURN OF SEIZED COMPUTER EQUIPMENT**

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes.